(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－134101
（P2003－134101A）
(43)公開日　平成15年５月９日(2003.5.9)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード*(参考)
Ｈ０４Ｌ　9/08		Ｇ０６Ｆ　12/14	３２０Ｂ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｇ０９Ｃ　1/00	６５０Ｚ	５Ｊ１０４
Ｇ０９Ｃ　1/00	６５０	Ｈ０４Ｌ　9/00	６０１Ａ	
Ｈ０４Ｌ　9/10			６０１Ｅ	
			６２１Ａ	

審査請求　未請求　請求項の数18　ＯＬ　（全 12 頁）

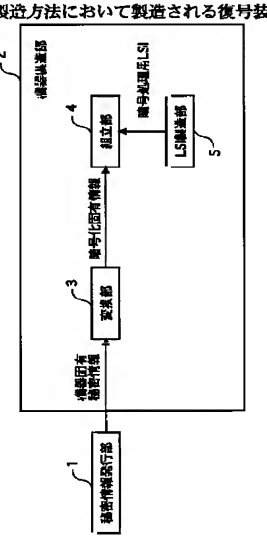
(21)出願番号　特願2002－212912(P2002－212912)
(22)出願日　平成14年７月22日(2002.7.22)
(31)優先権主張番号　特願2001－224126(P2001－224126)
(32)優先日　平成13年７月25日(2001.7.25)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　横田　薫
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　湯川　泰平
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100090446
弁理士　中島　司朗

最終頁に続く

(54)【発明の名称】　暗号処理用の素子とその暗号処理に用いる情報とを有する復号装置の製造方法、復号装置が有する情報と素子とを供給する供給システム、および前記製造方法において製造される復号装置。

(57)【要約】
【課題】　復号鍵を用いて復号処理を施す復号装置を製造する場合に、組立部において復号鍵のセキュリティを管理する特殊な環境が必要である。本発明は、組立部において特殊な環境の不必要な製造方法を提供することを目的とする。
【解決手段】　変換部３において、セキュリティが管理された状態で、復号鍵を秘密に取得して、取得された前記復号鍵に所定の暗号処理を施した暗号化復号鍵を含む変換情報を生成して出力する。組立部４において、出力された前記変換情報を前記復号装置に組み込まれるべき不揮発性メモリに書き込み、前記暗号化復号鍵に前記所定の暗号処理に対応する復号処理を施して前記復号鍵を得る回路と当該復号鍵を用いて復号処理を施す回路とが集積された１個の集積素子を含む前記復号装置を組み立てる。



【特許請求の範囲】
【請求項１】　復号鍵を用いて復号処理を施す復号装置の製造方法であって、
セキュリティが管理された状態において、前記復号鍵を秘密に取得する取得ステップと、
前記セキュリティが管理された状態において、取得された前記復号鍵に所定の暗号処理を施した暗号化復号鍵を含む変換情報を生成して出力する変換情報出力ステップと、
出力された前記変換情報を、前記復号装置に組み込まれるべき不揮発性メモリに書き込む書き込みステップと、
前記暗号化復号鍵に、前記所定の暗号処理に対応する復号処理を施して前記復号鍵を得る回路と当該復号鍵を用いて復号処理を施す回路とが集積された１個の集積素子を含む前記復号装置を組み立てる組み立てステップとを含むことを特徴とする製造方法。
【請求項２】　前記書き込みステップは、
前記セキュリティが管理された状態よりもセキュリティレベルの低い状態で実施されることを特徴とする請求項１に記載の製造方法。
【請求項３】　前記所定の暗号処理は、秘密鍵を用いた秘密鍵暗号方式であり、
前記変換情報出力ステップは、
所定の固定値の秘密鍵を用いて前記復号鍵に暗号処理を施すことを特徴とする請求項１に記載の製造方法。
【請求項４】　前記変換情報出力ステップは、
複数種類の暗号処理から１個を選択して、前記所定の暗号処理とする選択サブステップと、前記選択サブステップにより選択された前記所定の暗号処理を示す選択情報を生成する選択情報生成サブステップと、
前記復号鍵に前記所定の暗号処理を施して暗号化復号鍵を生成する暗号処理サブステップと、前記暗号化復号鍵と前記選択情報とを含む変換情報を生成する変換情報生成サブステップとを含み、
前記集積素子は、さらに、前記選択情報に基づいて、選択された前記所定の暗号処理を特定する特定回路を含むことを特徴とする請求項１に記載の製造方法。
【請求項５】　前記所定の暗号処理は、秘密鍵を用いた秘密鍵暗号方式であり、
前記選択サブステップは、
複数の秘密鍵から１個の秘密鍵を選択し、
前記選択情報生成サブステップは、
選択された前記秘密鍵を示す選択情報を生成し、
前記暗号処理サブステップは、
選択された前記秘密鍵を用いて、前記復号鍵に暗号処理を施して暗号化復号鍵を生成し、
前記変換情報生成サブステップは、
前記暗号化復号鍵と前記選択情報とを含む変換情報を生成し、
前記特定回路は、前記選択情報に基づいて、選択された前記秘密鍵を特定することを特徴とする請求項４に記載の製造方法。
【請求項６】　前記変換情報出力ステップは、さらに、
前記複数の秘密鍵を生成する鍵生成サブステップを含み、
前記選択サブステップは、
当該鍵生成サブステップにより生成された前記複数の秘密鍵から１個の前記秘密鍵を選択することを特徴とする請求項５に記載の製造方法。
【請求項７】　前記取得ステップは、
復号装置毎に固有の復号鍵を取得することを特徴とする請求項１に記載の製造方法。
【請求項８】　復号装置に書き込まれる情報を供給する情報供給装置と、当該復号装置に組み込まれる集積素子を供給する集積素子供給装置とからなる供給システムであって、
前記情報供給装置は、セキュリティの管理された状態で設けられ、
前記復号装置において復号処理に用いられる復号鍵を秘密に取得する取得手段と、
前記取得手段により取得された前記復号鍵に所定の暗号処理を施した暗号化復号鍵を含む変換情報を生成して、当該変換情報を前記復号装置を組み立てる組立部に出力する変換情報出力手段とを備え、
前記集積素子供給装置は、前記暗号化復号鍵に、前記所定の暗号処理に対応する復号処理を施して前記復号鍵を得る回路と、当該復号鍵を用いて復号処理を施す回路とが集積された１個の集積素子を製造する製造手段と、前記製造手段により製造された集積素子を前記組立部に供給する集積素子供給手段とを備えることを特徴とする供給システム。
【請求項９】　前記所定の暗号処理は、秘密鍵を用いた秘密鍵暗号方式であり、
前記変換情報出力手段は、
所定の固定値の秘密鍵を用いて前記復号鍵に暗号処理を施すことを特徴とする請求項８に記載の供給システム。
【請求項１０】　前記変換情報出力手段は、
複数種類の暗号処理から１個を選択して、前記所定の暗号処理とする選択手段と、
前記選択手段により選択された前記所定の暗号処理を示す選択情報を生成する選択情報生成手段と、
前記復号鍵に前記所定の暗号処理を施して暗号化復号鍵を生成する暗号処理手段と、
前記暗号化復号鍵と前記選択手段とを含む変換情報を生成する変換情報生成手段とを含み、
前記集積素子は、さらに、前記選択情報に基づいて、選択された前記所定の暗号処理を特定する特定回路を含むことを特徴とする請求項８に記載の供給システム。
【請求項１１】　前記所定の暗号処理は、秘密鍵を用いた秘密鍵暗号方式であり、

前記選択手段は、
複数の秘密鍵から１個の秘密鍵を選択し、
前記選択情報生成手段は、
選択された前記秘密鍵を示す選択情報を生成し、
前記暗号処理手段は、
選択された前記秘密鍵を用いて、前記復号鍵に暗号処理を施して暗号化復号鍵を生成し、
前記変換情報生成手段は、
前記暗号化復号鍵と前記選択手段とを含む変換情報を生成し、
前記特定回路は、前記選択情報に基づいて、選択された前記秘密鍵を特定することを特徴とする請求項１０に記載の供給システム。
【請求項１２】　前記変換情報出力手段は、さらに、
前記複数の秘密鍵を生成する鍵生成手段を含み、
前記選択手段は、
当該鍵生成手段により生成された前記複数の秘密鍵から１個の前記秘密鍵を選択することを特徴とする請求項１１に記載の供給システム。
【請求項１３】　前記取得手段は、
復号装置毎に固有の復号鍵を取得することを特徴とする請求項８に記載の供給システム。
【請求項１４】　復号鍵を用いて復号処理を施す復号装置であって、
前記復号鍵に、所定の暗号処理を施した暗号化復号鍵を含む変換情報が書き込まれている不揮発性メモリと、
前記暗号化復号鍵に、前記所定の暗号処理に対応する復号処理を施して前記復号鍵を得る回路と当該復号鍵を用いて復号処理を施す回路とを含む１個の集積素子とを備えることを特徴とする復号装置。
【請求項１５】　前記所定の暗号処理は、秘密鍵を用いた秘密鍵暗号方式であり、
前記不揮発性メモリは、
所定の固定値の秘密鍵を用いて、前記復号鍵に秘密鍵暗号方式の暗号処理を施した暗号化復号鍵を含む変換情報が書き込まれており、
前記集積素子は、
前記暗号化復号鍵に、前記秘密鍵を用いて復号処理を施して前記復号鍵を得る回路と当該復号鍵を用いて復号処理を施す回路とを含むことを特徴とする請求項１４に記載の復号装置。
【請求項１６】　前記不揮発性メモリは、
複数種類の暗号処理から１個を選択して前記所定の暗号処理とし、選択された前記所定の暗号処理を示す選択情報と前記暗号化復号鍵とを含む変換情報が書き込まれており、
前記集積素子は、さらに、前記選択情報に基づいて、選択された前記所定の暗号処理を特定する特定回路を含むことを特徴とする請求項１４に記載の復号装置。
【請求項１７】　前記所定の暗号処理は、秘密鍵を用いた秘密鍵暗号方式であり、
前記不揮発性メモリは、
複数の秘密鍵から１個の秘密鍵を選択し、選択された前記秘密鍵を示す選択情報と、前記秘密鍵を用いて秘密鍵暗号方式の暗号処理を施した暗号化復号鍵とを含む変換情報が書き込まれており、
前記集積素子は、前記選択情報に基づいて、選択された前記秘密鍵を特定する前記特定回路を含むことを特徴とする請求項１６に記載の復号装置。
【請求項１８】　前記不揮発性メモリは、
復号装置毎に固有の復号鍵に、所定の暗号処理を施した暗号化復号鍵を含む変換情報が書き込まれていることを特徴とする請求項１４に記載の復号装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、著作権保護機能を持つＡＶディジタル機器などのように、暗号処理用の素子とその暗号処理に用いる情報とを有する復号装置の製造方法、復号装置が有する情報と素子とを供給する供給システム、および前記製造方法において製造される復号装置に関する。
【０００２】
【従来の技術】近年、映画や音楽などのＡＶコンテンツのディジタル化が進み、映画や音楽などの有料コンテンツ配信サービスや、ディジタル放送の限定放送といった各種サービスが実現されている。そういったサービスを実現するためには、配信あるいは放送するＡＶコンテンツに対して暗号処理を施して不正な視聴を防止する必要がある。例えば、ＡＶコンテンツを記録媒体に記録させて配布する場合や、インターネットや放送網などによってＡＶコンテンツを配信する場合には、記録あるいは配信されるＡＶコンテンツは暗号化される。この暗号化されたＡＶコンテンツは、視聴料を払った特定のユーザまたは視聴者だけが復号化でき再生できる仕組みとなっている。
【０００３】上記の仕組みを実現する再生機器は、暗号化されたコンテンツの復号化などを行うための暗号処理回路と鍵情報とを備える必要がある。このような再生機器の製造過程においては、通常のＡＶデコーダ機器の製造工程に加えて、暗号処理回路の製造、及び暗号処理に用いる鍵情報の書き込み、といった工程が必要である。
【０００４】図７は記録媒体を利用した有料コンテンツ配布方式の構成を示す図である。有料コンテンツ記録媒体１５は、例えば光ディスクといった大容量のディジタルコンテンツデータを記録できる記録媒体であり、暗号化コンテンツ鍵データを記録する暗号化コンテンツ鍵データ記録領域１７と暗号化コンテンツデータを記録する暗号化コンテンツデータ記録領域１８とを備える。暗号化コンテンツ鍵データは、有料コンテンツを購入したユーザが有する再生機器に固有の機器固有秘密情報を用い

て、コンテンツ鍵を暗号化することで得られ、暗号化コンテンツデータは、コンテンツ鍵データを用いてコンテンツデータを暗号化することで得られる。また、有料コンテンツ再生機器１６は、有料コンテンツ記録媒体１５に記録されている有料コンテンツデータを再生するための再生機器であり、暗号処理に必要な機器固有秘密情報を記録する不揮発性メモリ１９と、有料コンテンツデータを復号化するための暗号処理を行う暗号処理用ＬＳＩ２０とを備える。ここで、機器固有秘密情報とは、機器ごとに固有な秘密情報として与えられるものである。有料コンテンツ再生機器１６が、有料コンテンツ記録媒体１５に記録されている有料コンテンツデータを再生する際の処理は以下の通りである。

【０００５】まず、暗号処理用ＬＳＩ２０は、暗号化コンテンツ鍵データ記録領域１７から暗号化コンテンツ鍵データ、そして暗号化コンテンツデータ記録領域１８から暗号化コンテンツデータを読み出す。さらに暗号処理用ＬＳＩ２０が、不揮発性メモリ１９に記録された機器固有秘密情報を用いて、一連の復号処理を行って暗号化コンテンツデータを復号化する。

【０００６】有料コンテンツ再生機器１６内において、暗号化コンテンツを復号化するには、コンテンツ鍵データが必要である。そのコンテンツ鍵データを復号化するには機器固有秘密情報が必要がある。したがって有料コンテンツを購入したユーザが所有する有料コンテンツ再生機器１６だけが有料コンテンツを再生することができ、他のユーザの不正な再生が防止される。

【０００７】図８はインターネットや放送網を利用した有料コンテンツ配信方式の構成を示す図である。図７の例で有料コンテンツ記録媒体１５から読み出していた暗号化コンテンツ鍵データ及び暗号化コンテンツデータは、図８の例では有料コンテンツ配信局２１の有料コンテンツ配信手段２３から通信路を介して有料コンテンツ再生機器２２に伝送される。有料コンテンツ配信局２１は、インターネットを利用した有料コンテンツ配信の場合には、コンテンツプロバイダであり、放送網を利用した配信の場合には、放送局である。また、図８の場合の有料コンテンツ再生機器２２は、有料コンテンツを購入したユーザが受信した有料コンテンツを再生するためのＰＣあるいはディジタルセットトップボックスなどのことである。暗号化コンテンツ鍵データ及び暗号化コンテンツデータを受信した後の処理は、図７の例における有料コンテンツ再生機器１６の処理と同様である。

【０００８】図９は図８の有料コンテンツ再生機器２２に含まれる暗号処理用ＬＳＩ２５の内部構成を示す図である。暗号処理用ＬＳＩ２５はコンテンツ鍵復号回路２５１とコンテンツ復号回路２５２とを含む。図９を用いて、暗号処理用ＬＳＩ２５の処理について説明する。まず、暗号化コンテンツ鍵復号回路２５１は、不揮発性メモリ２４から読み出した機器固有秘密情報を用いて、外部から入力される暗号化コンテンツ鍵データに対して所定の復号処理を行い、コンテンツ鍵を得る。そして、コンテンツ復号回路２５２は、そのコンテンツ鍵を用いて外部から入力される暗号化コンテンツデータを復号化する。

【０００９】図１０は不揮発性メモリと暗号処理用ＬＳＩとを備える有料コンテンツ再生機器の製造方法に関する従来の構成を示す図である。秘密情報発行部２６は、有料コンテンツ再生機器に実装するための暗号技術の使用を機器製造部２７に許可するライセンス機関により運営されている。秘密情報発行部２６により発行された機器固有秘密情報は、秘密に、機器の製造を許可された機器製造部２７に送付される。図１０の機器製造部２７は、組立部２７１とＬＳＩ製造部２７２とを備える。組立部２７１は、送付された機器固有秘密情報を、不揮発性メモリ２４に書き込む。この不揮発性メモリ２４は、ＬＳＩ製造部２７２で製造された暗号処理用ＬＳＩ２５などと共に組立てられて、有料コンテンツ再生機器が製造される。なお、有料コンテンツ再生機器には、上記の他にＡＶコンテンツデータの復号などに必要な回路が組み込まれているが、それらは本発明とは直接関係がないのでここでは割愛している。

【００１０】また、機器固有秘密情報は、不正利用を防止するため、発行されてから完成品として組み立てられるまで機密性が保持されなければならない。したがって組立部２７１において、施錠可能なドアと仕切りによって区切られた作業スペースを確保し、その中での作業者をごく限られた者だけに限定する等の措置が行われる。

【発明が解決しようとする課題】しかしながら、このような措置は上記の特殊な環境を構築するための費用がかかり、また作業者も限定されるので生産性が低下するという問題がある。さらに、一般に組立部は、機種ごとに異なる工場に置かれることが多い。そのため、上記の特殊な環境の構築はそれぞれの工場で必要となり、構築費用はますます増大してしまうという問題がある。

【００１１】本発明は、特殊な環境の構築費用の増大や生産性の低下を防ぎ、機器固有秘密情報を有する有料コンテンツ再生機器を製造する製造方法、有料コンテンツ再生機器に機器固有秘密情報とＬＳＩとを供給する供給システムおよび前記製造方法において製造される有料コンテンツ再生機器を提供することを目的とする。

【００１２】

【課題を解決するための手段】上記目的を達成する製造方法は、復号鍵を用いて復号処理を施す復号装置の製造方法であって、セキュリティが管理された状態において前記復号鍵を秘密に取得する取得ステップと、前記セキュリティが管理された状態において、取得された前記復号鍵に所定の暗号処理を施した暗号化復号鍵を含む変換情報を生成して出力する変換情報出力ステップと、出力された前記変換情報を、前記復号装置に組み込まれるべ

き不揮発性メモリに書き込む書き込みステップと、前記暗号化復号鍵に、前記所定の暗号処理に対応する復号処理を施して前記復号鍵を得る回路と当該復号鍵を用いて復号処理を施す回路とが集積された１個の集積素子を含む前記復号装置を組み立てる組み立てステップとを含むことを特徴とする。

【００１３】この構成によれば、復号鍵をそのまま使用せず、一旦暗号処理を施した暗号化復号鍵が、書き込みステップと組み立てステップとにおいて使用されている。それゆえこれらのステップは、セキュリティの管理された場所において実施する必要がない。また、素子内部にて復号処理を施された復号鍵は、素子の外部に出力されることがないので機密性は保持される。

【００１４】したがって、書き込みステップと組み立てステップとを含む復号装置の組立部において、復号鍵の機密性を保持するための特殊な環境を構築するための費用の増大と、作業者が限定されることによる生産性の低下とを防ぐ製造方法を提供することができる。また、上記目的を達成する供給システムは、復号装置に書き込まれる情報を供給する情報供給装置と、当該復号装置に組み込まれる集積素子を供給する集積素子供給装置とからなる供給システムであって、前記情報供給装置は、セキュリティの管理された状態で設けられ、前記復号装置において復号処理に用いられる復号鍵を秘密に取得する取得手段と、前記取得手段により取得された前記復号鍵に所定の暗号処理を施した暗号化復号鍵を含む変換情報を生成して、当該変換情報を前記復号装置を組み立てる組立部に出力する変換情報出力手段とを備え、前記集積素子供給装置は、前記暗号化復号鍵に前記所定の暗号処理に対応する復号処理を施して前記復号鍵を得る回路と、当該復号鍵を用いて復号処理を施す回路とが集積された１個の集積素子を製造する製造手段と、前記製造手段により製造された集積素子を前記組立部に供給する集積素子供給手段とを備えることを特徴とする。

【００１５】この構成によれば、情報供給装置は、セキュリティの管理された場所に設けられ、復号鍵に一旦暗号処理を施して暗号化復号鍵を生成する。その暗号鍵復号鍵は変換情報に含められて組立部に供給される。したがって、復号装置の組立部において、復号鍵の機密性を保持するための特殊な環境を構築するための費用の増大と、作業者が限定されることによる生産性の低下とを防ぐ供給システムを提供することができる。

【００１６】また、上記目的を達成する復号装置は、復号鍵を用いて復号処理を施す復号装置であって、前記復号鍵に、所定の暗号処理を施した暗号化復号鍵を含む変換情報が書き込まれている不揮発性メモリと、前記暗号化復号鍵に、前記所定の暗号処理に対応する復号処理を施して前記復号鍵を得る回路と当該復号鍵を用いて復号処理を施す回路とを含む１個の集積素子とを備えることを特徴とする。

【００１７】この構成によれば、復号鍵をそのまま扱わず、一旦暗号処理を施した暗号化復号鍵を扱うことで、装置の組み立て時に、セキュリティの管理された場所において実施する必要がない。また、素子内部にて復号処理を施された復号鍵は、素子の外部に出力されることがないので機密性は保持される。したがって、復号装置の組立部において、復号鍵の機密性を保持するための特殊な環境を構築するための費用の増大と、作業者が限定されることによる生産性の低下とを防ぐことができる。

【００１８】

【発明の実施の形態】（実施の形態１）図１は本発明における機器固有秘密情報を有する有料コンテンツ再生機器の製造方法に関する実施の形態１の構成を示す図である。秘密情報発行部１は、機器製造の許可を受けた機器製造部２に機器固有秘密情報を発行して送付する。

【００１９】機器製造部２は、機器固有秘密情報を有する有料コンテンツ再生機器を製造し、変換部３、組立部４およびＬＳＩ製造部５を備える。変換部３は、セキュリティの管理された場所で、機器固有秘密情報に対して所定の暗号処理を施して暗号化固有情報を生成する。生成された暗号化固有情報は組立部４に送付される。

【００２０】ここで、セキュリティの管理された場所とは、施錠可能なドアと仕切りによって区切られた作業スペースのような、機密性の保持された場所を指す。また、所定の暗号処理としては、ＤＥＳ（Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）暗号の６４ビット（パリティビット８ビットを含む）の秘密鍵を用いた暗号処理を用いる。なお、ＤＥＳについては、例えば、岡本栄司著「暗号理論入門」（共立出版）に詳しく書かれている。

【００２１】組立部４は、送付された暗号化固有情報を不揮発性メモリに書き込み、ＬＳＩ製造部５で製造された暗号処理用ＬＳＩなどを組み立てて、有料コンテンツ再生機器を製造する。図２は有料コンテンツを再生する場合の不揮発性メモリと暗号処理用ＬＳＩとの構成を示す図である。

【００２２】不揮発性メモリ６は、組立部４において暗号化固有情報が書き込まれ、暗号処理用ＬＳＩ７と接続されて有料コンテンツ再生機器に組み込まれる。暗号処理用ＬＳＩ７は、ＬＳＩ製造部５において製造されたもので、秘密情報復号回路７１、コンテンツ鍵復号回路７２およびコンテンツ復号回路７３を有し、機器固有秘密情報を復号鍵として送付される暗号化コンテンツ鍵データを復号化し、さらに当該コンテンツ鍵を用いて、暗号化コンテンツデータを復号化する。

【００２３】秘密情報復号回路７１は、変換部３において機器固有秘密情報に施した所定の暗号処理に対応する復号処理を行う回路である。これによって、暗号化固有情報は機器固有秘密情報に復号化される。具体的には、６４ビット（パリティ８ビットを含む）の秘密鍵を用い

たＤＥＳ暗号の復号処理を用い、秘密鍵は変換部３で用いられている暗号処理と同じものを用いる。

【００２４】コンテンツ鍵復号回路７２は、秘密情報復号回路７１で復号化されて得た機器固有秘密情報を用いて、外部から入力される暗号化コンテンツ鍵データに対する復号処理を行う。コンテンツ復号回路７３は、コンテンツ鍵復号回路７２で復号化されたコンテンツ鍵を用いて、外部から入力される暗号化コンテンツデータを復号化してコンテンツデータを得る。

【００２５】図３は本発明における機器固有秘密情報を有する有料コンテンツ再生機器の製造工程の手順を示す図である。次に実施の形態１における有料コンテンツ再生機器の製造工程の手順を図３を用いて説明する。秘密情報発行部１が、機器製造の許可を受けた機器製造部２に機器固有秘密情報を発行して送付する（ステップ：Ｓ１１）。

【００２６】変換部３が、セキュリティの管理された場所で、送付された機器固有秘密情報を秘密に取得し（ステップ：Ｓ１２）、機器固有秘密情報に対して所定の暗号処理を施して暗号化固有情報を生成する（ステップ：Ｓ１３）。生成された暗号化固有情報は組立部４に送付される。組立部４が、送付された暗号化固有情報を不揮発性メモリに書き込み（ステップ：Ｓ１４）、ＬＳＩ製造部５で製造された暗号処理用ＬＳＩなどを組み立てて（ステップ：Ｓ１５）、有料コンテンツ再生機器を製造する。

【００２７】実施の形態１では、変換部３において変換された暗号化固有情報は、秘密情報復号回路７１において元の機器固有秘密情報に復号化され、コンテンツ鍵復号回路７２に入力される。したがって、暗号化コンテンツ鍵データの復号処理は、秘密情報発行部１で発行された機器固有秘密情報と同じものを用いて行われるので、以降のコンテンツ復号処理は正しく行われる。

【００２８】また、機器固有秘密情報は、暗号化固有情報の状態で組立部４に送付される。暗号化固有情報は、所定の暗号処理により変換された後のデータであるから、機器固有秘密情報のように機密性を保持する必要はない。したがって、組立部４において、不揮発性メモリに書き込み、及び組み立て作業の際に機密性を保持するための特殊な環境を構築する必要がない。即ち、組立部４における特殊な環境の構築費用の増大や生産性の低下は生じない。

【００２９】（実施の形態２）図４は本発明における機器固有秘密情報を有する有料コンテンツ再生機器の製造方法に関する実施の形態２の構成を示す図である。実施の形態２では、変換部１０において所定の暗号処理が複数種類の暗号処理から選択されたものであることが特徴となっており、その他については実施の形態１と同様であるので説明を省略する。

【００３０】秘密情報発行部８は、機器製造部９に機器固有秘密情報を送付する。機器製造部９は、変換部１０、組立部１１およびＬＳＩ製造部１２を備える。変換部１０は、セキュリティの管理された場所において、機器固有秘密情報に複数種類の暗号処理のいずれかの暗号処理を施して暗号化固有情報を生成する。変換部１０は、さらに、いずれの変換を選んだかを示すパラメータ情報と暗号化固有情報とを組立部１１に送付する。具体的には、複数種類の暗号処理は、生成された６４ビットの秘密鍵を１６種類選んだＤＥＳ暗号の暗号処理とし、それぞれの秘密鍵に１から１６までの番号を割り当て、この番号をパラメータ情報とする。

【００３１】組立部１１は、変換部１０から送付された暗号化固有情報とパラメータ情報とを不揮発性メモリに書き込み、ＬＳＩ製造部１２で製造された暗号処理用ＬＳＩなどを組み立てて、有料コンテンツ再生機器を製造する。図５は有料コンテンツを再生する場合の不揮発性メモリと暗号処理用ＬＳＩとの構成を示す図である。

【００３２】不揮発性メモリ１３は、暗号化固有情報とパラメータ情報とが書き込まれ、暗号処理用ＬＳＩ１４と接続されて有料コンテンツ再生機器に組み込まれる。暗号処理用ＬＳＩ１４は、ＬＳＩ製造部１２において製造されたもので、パラメータ記憶手段１４１、秘密情報復号回路１４２、コンテンツ鍵復号回路１４３及びコンテンツ復号回路１４４を有する。

【００３３】パラメータ記憶手段１４１は、変換部１０が有する複数種類の暗号処理のそれぞれに対応したパラメータ情報を記憶している。具体的には、先ほど述べた１６種類の秘密鍵を用いたＤＥＳ暗号の復号処理と１から１６の番号とを対応させた形で記録している。秘密情報復号回路１４２は、不揮発性メモリ１３から暗号化固有情報とパラメータ情報とを読み取り、パラメータ情報を元に選んだ復号処理を暗号化固有情報に施すことによって、機器固有秘密情報を得る。

【００３４】図６は本発明における機器固有秘密情報を有する有料コンテンツ再生機器の製造工程の手順を示す図である。次に実施の形態２における有料コンテンツ再生機器の製造工程の手順を図６を用いて説明する。秘密情報発行部８が、機器製造の許可を受けた機器製造部９に機器固有秘密情報を発行して送付する（ステップ：Ｓ２１）。

【００３５】変換部１０が、セキュリティの管理された場所で、送付された機器固有秘密情報を秘密に取得する（ステップ：Ｓ２２）。さらに変換部１０が、複数種類の暗号処理の中からいずれかを選択し（ステップ：Ｓ２３）、機器固有秘密情報に対して選択された暗号処理を施して暗号化固有情報を生成する（ステップ：Ｓ２４）。その後、選択された所定の暗号処理を示すパラメータ情報と生成された暗号化固有情報とが、組立部１１に送付される。

【００３６】組立部１１が、送付されたパラメータ情報

と暗号化固有情報とを不揮発性メモリ１３に書き込み（ステップ：Ｓ２５）、ＬＳＩ製造部１２で製造された暗号処理用ＬＳＩなどを組み立てて（ステップ：Ｓ２６）、有料コンテンツ再生機器を製造する。実施の形態２においても、実施の形態１と同様、機密性を保持する必要のある機器固有秘密情報は、暗号化固有情報に変換されて組立部１１に送付されるので、組立部１１において機密性を保持するための特殊な環境の必要がない。したがって、特殊な環境を構築する費用の増大や生産性の低下は生じない。また、機器固有秘密情報の暗号処理が固定的でなく、同じ機器固有秘密情報であっても選択する暗号処理を変えることで暗号化固有情報を異ならせることができるので、実施の形態１よりも機器固有秘密情報の機密性が向上している。

【００３７】なお、実施の形態１において、変換部３において用いる所定の暗号処理は、６４ビットの秘密鍵を用いたＤＥＳ暗号処理を用い、その暗号処理に対応する復号処理は、同じ固定鍵を用いたＤＥＳ復号処理を用いているが、これは暗号処理と復号処理との関係にある変換であれば何でもよい。同様に、実施の形態２において、変換部１０において用いる複数種類の所定の暗号処理は、１６種類の６４ビットの秘密鍵を用いたＤＥＳ暗号処理を用いているが、これも暗号処理と復号処理との関係にある変換であれば何でもよい。また、暗号処理の個数は１６個に限定されないことはいうまでもない。

【００３８】さらに、実施の形態２において、変換部１０において用いる複数種類の暗号処理は、１６種類の秘密鍵を用いたＤＥＳ暗号変換を用いているが、この１６種類の秘密鍵は、予め決めた固定の値とする必要はなく、例えば、ＬＳＩのロットが変わる毎に異なる鍵を用いてもよい。また、実施の形態１および実施の形態２において、機器製造部にある組立部は、１つだけの構成となっているが、これは複数あってもよい。さらに、変換部やＬＳＩ製造部も１つだけである必要はなく、これらも複数あってもよい。

【００３９】また、実施の形態１および実施の形態２において、機器製造部に変換部、組立部およびＬＳＩ製造部がある構成になっているが、この構成に限られるものではない。例えば、機器の組み立てを行う組立会社とＬＳＩ製造を行うＬＳＩ製造会社との２つの会社に分かれている場合には、ＬＳＩ製造会社に変換部とＬＳＩ製造部とがあり、ＬＳＩ製造会社は暗号化固有情報と暗号処理用ＬＳＩとを組立会社に送付し、組立会社において、暗号化固有情報を不揮発性メモリに書き込み、暗号処理用ＬＳＩなどと組み立てるという構成でもよい。

【００４０】この場合には、ＬＳＩ製造会社から送付される暗号化固有情報は機密性を保持する必要がないので、組立会社では、機密性を保持する特殊な環境を構築せずに組立が行える。また、このときＬＳＩ製造会社や組立会社は複数あってもよい。なお、実施の形態１および実施の形態２において、不揮発性メモリは、いわゆるＲＯＭだけのことを指すのではなく、ハードロジック、印刷パターン、ヒューズなどの様にデータを蓄える場合に揮発性のものではないことを指す。

【００４１】

【発明の効果】本発明に係る製造方法は、復号鍵を用いて復号処理を施す復号装置の製造方法であって、セキュリティが管理された状態において、前記復号鍵を秘密に取得する取得ステップと、前記セキュリティが管理された状態において、取得された前記復号鍵に所定の暗号処理を施した暗号化復号鍵を含む変換情報を生成して出力する変換情報出力ステップと、出力された前記変換情報を、前記復号装置に組み込まれるべき不揮発性メモリに書き込む書き込みステップと、前記暗号化復号鍵に、前記所定の暗号処理に対応する復号処理を施して前記復号鍵を得る回路と当該復号鍵を用いて復号処理を施す回路とが集積された１個の集積素子を含む前記復号装置を組み立てる組み立てステップとを含むことを特徴とする。

【００４２】この構成によれば、復号鍵をそのまま使用せず、一旦暗号処理を施した暗号化復号鍵が、書き込みステップと組み立てステップとにおいて使用されている。それゆえこれらのステップは、セキュリティの管理された場所において実施する必要がない。また、素子内部にて復号処理を施された復号鍵は、素子の外部に出力されることがないので機密性は保持される。

【００４３】したがって、書き込みステップと組み立てステップとを含む復号装置の組立部において、復号鍵の機密性を保持するための特殊な環境を構築するための費用の増大と、作業者が限定されることによる生産性の低下とを防ぐ製造方法を提供することができる。また、前記書き込みステップは、前記セキュリティが管理された状態よりもセキュリティレベルの低い状態で実施されてもよい。

【００４４】このように機密性の必要なところと不必要なところとを差別化することで、復号装置の組立部において、復号鍵の機密性を保持するための特殊な環境を構築するための費用の増大と、作業者が限定されることによる生産性の低下とがない製造方法を実現することができる。また、前記所定の暗号処理は、秘密鍵を用いた秘密鍵暗号方式であり、前記変換情報出力ステップは、所定の固定値の秘密鍵を用いて前記復号鍵に暗号処理を施すこととしてもよい。

【００４５】このように、秘密鍵暗号方式を採用することにより、公開鍵暗号方式に比べて暗号化および復号化にかかる処理の単純化を図ることができる。また、前記変換情報出力ステップは、複数種類の暗号処理から１個を選択して、前記所定の暗号処理とする選択サブステップと、前記選択サブステップにより選択された前記所定の暗号処理を示す選択情報を生成する選択情報生成サブステップと、前記復号鍵に前記所定の暗号処理を施して

暗号化復号鍵を生成する暗号処理サブステップと、前記暗号化復号鍵と前記選択情報とを含む変換情報を生成する変換情報生成サブステップとを含み、前記集積素子は、さらに、前記選択情報に基づいて、選択された前記所定の暗号処理を特定する特定回路を含むこととしてもよい。

【００４６】このように、復号鍵は複数種類の暗号処理のいずれか１個の暗号処理を施される。したがって、暗号処理が１種類だけの場合に比べて復号鍵の機密性を高めることができる。また、選択情報を変換情報に含めて不揮発性メモリに書き込むことで、素子は、復号鍵が複数種類の暗号処理のいずれを用いて変換されたかを特定することができる。

【００４７】また、前記所定の暗号処理は、秘密鍵を用いた秘密鍵暗号方式であり、前記選択サブステップは、複数の秘密鍵から１個の秘密鍵を選択し、前記選択情報生成サブステップは、選択された前記秘密鍵を示す選択情報を生成し、前記暗号処理サブステップは、選択された前記秘密鍵を用いて、前記復号鍵に暗号処理を施して暗号化復号鍵を生成し、前記変換情報生成サブステップは、前記暗号化復号鍵と前記選択情報とを含む変換情報を生成し、前記特定回路は、前記選択情報に基づいて、選択された前記秘密鍵を特定することとしてもよい。

【００４８】このように、秘密鍵暗号方式を採用することにより、公開鍵暗号方式に比べて暗号化および復号化にかかる処理の単純化を図ることができる。また、選択情報を変換情報に含めて不揮発性メモリに書き込むことで、素子は、復号鍵が複数種類の暗号処理のいずれを用いて変換されたかを特定することができる。

【００４９】また、前記変換情報出力ステップは、さらに、前記複数の秘密鍵を生成する鍵生成サブステップを含み、前記選択サブステップは、当該鍵生成サブステップにより生成された前記複数の秘密鍵から１個の前記秘密鍵を選択することとしてもよい。これによって複数の秘密鍵を生成することができる。また、秘密鍵を変更することができるので、機密性が向上する。

【００５０】また、前記取得ステップは、復号装置毎に固有の復号鍵を取得することとしてもよい。このように、復号鍵は復号装置毎に個々に割り当てられ、復号装置と復号鍵とを１対１で対応させることができる。また、本発明に係る供給システムは、復号装置に書き込まれる情報を供給する情報供給装置と、当該復号装置に組み込まれる集積素子を供給する集積素子供給装置とからなる供給システムであって、前記情報供給装置は、セキュリティの管理された状態で設けられ、前記復号装置において復号処理に用いられる復号鍵を秘密に取得する取得手段と、前記取得手段により取得された前記復号鍵に所定の暗号処理を施した暗号化復号鍵を含む変換情報を生成して、当該変換情報を前記復号装置を組み立てる組立部に出力する変換情報出力手段とを備え、前記集積素子供給装置は、前記暗号化復号鍵に、前記所定の暗号処理に対応する復号処理を施して前記復号鍵を得る回路と、当該復号鍵を用いて復号処理を施す回路とが集積された１個の集積素子を製造する製造手段と、前記製造手段により製造された集積素子を前記組立部に供給する集積素子供給手段とを備えることを特徴とする。

【００５１】この構成によれば、情報供給装置は、セキュリティの管理された場所に設けられ、復号鍵に一旦暗号処理を施して暗号化復号鍵を生成する。その暗号鍵復号鍵は変換情報に含められて組立部に供給される。したがって、復号装置の組立部において、復号鍵の機密性を保持するための特殊な環境を構築するための費用の増大と、作業者が限定されることによる生産性の低下とを防ぐ供給システムを提供することができる。

【００５２】また、前記所定の暗号処理は、秘密鍵を用いた秘密鍵暗号方式であり、前記変換情報出力手段は、所定の固定値の秘密鍵を用いて前記復号鍵に暗号処理を施すこととしてもよい。このように、秘密鍵暗号方式を採用することにより、公開鍵暗号方式に比べて暗号化および復号化にかかる処理の単純化を図ることができる。また、前記変換情報出力手段は、複数種類の暗号処理から１個を選択して、前記所定の暗号処理とする選択手段と、前記選択手段により選択された前記所定の暗号処理を示す選択情報を生成する選択情報生成手段と、前記復号鍵に前記所定の暗号処理を施して暗号化復号鍵を生成する暗号処理手段と、前記暗号化復号鍵と前記選択手段とを含む変換情報を生成する変換情報生成手段とを含み、前記集積素子は、さらに、前記選択情報に基づいて、選択された前記所定の暗号処理を特定する特定回路を含むこととしてもよい。

【００５３】このように、復号鍵は複数種類の暗号処理のいずれか１個の暗号処理を施される。したがって、暗号処理が１種類だけの場合に比べて復号鍵の機密性を高めることができる。また、選択情報を変換情報に含めて不揮発性メモリに書き込むことで、素子は、復号鍵が複数種類の暗号処理のいずれを用いて変換されたかを特定することができる。

【００５４】また、前記所定の暗号処理は、秘密鍵を用いた秘密鍵暗号方式であり、前記選択手段は、複数の秘密鍵から１個の秘密鍵を選択し、前記選択情報生成手段は、選択された前記秘密鍵を示す選択情報を生成し、前記暗号処理手段は、選択された前記秘密鍵を用いて、前記復号鍵に暗号処理を施して暗号化復号鍵を生成し、前記変換情報生成手段は、前記暗号化復号鍵と前記選択手段とを含む変換情報を生成し、前記特定回路は、前記選択情報に基づいて、選択された前記秘密鍵を特定することとしてもよい。

【００５５】このように、秘密鍵暗号方式を採用することにより、公開鍵暗号方式に比べて暗号化および復号化にかかる処理の単純化を図ることができる。また、選択

情報を変換情報に含めて不揮発性メモリに書き込むことで、素子は、復号鍵が複数種類の暗号処理のいずれを用いて変換されたかを特定することができる。

【００５６】また、前記変換情報出力手段は、さらに、前記複数の秘密鍵を生成する鍵生成手段を含み、前記選択手段は、当該鍵生成手段により生成された前記複数の秘密鍵から１個の前記秘密鍵を選択することとしてもよい。これによって複数の秘密鍵を生成することができる。また、秘密鍵を変更することができるので、機密性が向上する。

【００５７】また、前記取得手段は、復号装置毎に固有の復号鍵を取得することとしてもよい。このように、復号鍵は復号装置毎に個々に割り当てられ、復号装置と復号鍵とを１対１で対応させることができる。また、本発明に係る復号装置は、復号鍵を用いて復号処理を施す復号装置であって、前記復号鍵に、所定の暗号処理を施した暗号化復号鍵を含む変換情報が書き込まれている不揮発性メモリと、前記暗号化復号鍵に、前記所定の暗号処理に対応する復号処理を施して前記復号鍵を得る回路と当該復号鍵を用いて復号処理を施す回路とを含む１個の集積素子とを備えることを特徴とする。

【００５８】この構成によれば、復号鍵をそのまま扱わず、一旦暗号処理を施した暗号化復号鍵を扱うことで、装置の組み立て時に、セキュリティの管理された場所において実施する必要がない。また、素子内部にて復号処理を施された復号鍵は、素子の外部に出力されることがないので機密性は保持される。したがって、復号装置の組立部において、復号鍵の機密性を保持するための特殊な環境を構築するための費用の増大と、作業者が限定されることによる生産性の低下とを防ぐことができる。

【００５９】また、前記所定の暗号処理は、秘密鍵を用いた秘密鍵暗号方式であり、前記不揮発性メモリは、所定の固定値の秘密鍵を用いて、前記復号鍵に秘密鍵暗号方式の暗号処理を施した暗号化復号鍵を含む変換情報が書き込まれており、前記集積素子は、前記暗号化復号鍵に、前記秘密鍵を用いて復号処理を施して前記復号鍵を得る回路と当該復号鍵を用いて復号処理を施す回路とを含むこととしてもよい。

【００６０】このように、秘密鍵暗号方式を採用することにより、公開鍵暗号方式に比べて暗号化および復号化にかかる処理の単純化を図ることができる。また、前記不揮発性メモリは、複数種類の暗号処理から１個を選択して前記所定の暗号処理とし、選択された前記所定の暗号処理を示す選択情報と前記暗号化復号鍵とを含む変換情報が書き込まれており、前記集積素子は、さらに、前記選択情報に基づいて、選択された前記所定の暗号処理を特定する特定回路を含むこととしてもよい。

【００６１】このように、復号鍵は複数種類の暗号処理のいずれか１個の暗号処理を施される。したがって、暗号処理が１種類だけの場合に比べて復号鍵の機密性を高めることができる。また、選択情報を変換情報に含めて不揮発性メモリに書き込むことで、素子は、復号鍵が複数種類の暗号処理のいずれを用いて変換されたかを特定することができる。

【００６２】また、前記所定の暗号処理は、秘密鍵を用いた秘密鍵暗号方式であり、前記不揮発性メモリは、複数の秘密鍵から１個の秘密鍵を選択し、選択された前記秘密鍵を示す選択情報と、前記秘密鍵を用いて秘密鍵暗号方式の暗号処理を施した暗号化復号鍵とを含む変換情報が書き込まれており、前記集積素子は、前記選択情報に基づいて、選択された前記秘密鍵を特定する前記特定回路を含むこととしてもよい。

【００６３】このように、秘密鍵暗号方式を採用することにより、公開鍵暗号方式に比べて暗号化および復号化にかかる処理の単純化を図ることができる。また、選択情報を変換情報に含めて不揮発性メモリに書き込むことで、素子は、復号鍵が複数種類の暗号処理のいずれを用いて変換されたかを特定することができる。

【００６４】また、前記不揮発性メモリは、復号装置毎に固有の復号鍵に、所定の暗号処理を施した暗号化復号鍵を含む変換情報が書き込まれていることとしてもよい。このように、復号鍵は復号装置毎に個々に割り当てられ、復号装置と復号鍵とを１対１で対応させることができる。

【図面の簡単な説明】

【図１】本発明における機器固有秘密情報を有する有料コンテンツ再生機器の製造方法に関する実施の形態１の構成を示す図である。

【図２】有料コンテンツを再生する場合の不揮発性メモリと暗号処理用ＬＳＩとの構成を示す図である。

【図３】本発明における機器固有秘密情報を有する有料コンテンツ再生機器の製造工程の手順を示す図である。

【図４】本発明における機器固有秘密情報を有する有料コンテンツ再生機器の製造方法に関する実施の形態２の構成を示す図である。

【図５】有料コンテンツを再生する場合の不揮発性メモリと暗号処理用ＬＳＩとの構成を示す図である。

【図６】本発明における機器固有秘密情報を有する有料コンテンツ再生機器の製造工程の手順を示す図である。

【図７】記録媒体を利用した有料コンテンツ配布方式の構成を示す図である。

【図８】インターネットや放送網を利用した有料コンテンツ配信方式の構成を示す図である。

【図９】暗号処理用ＬＳＩ２５の内部構成を示す図である。

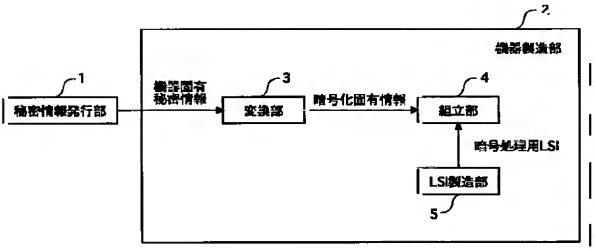
【図１０】不揮発性メモリと暗号処理用ＬＳＩとを備える有料コンテンツ再生機器の製造方法に関する従来の構成を示す図である。

【符号の説明】

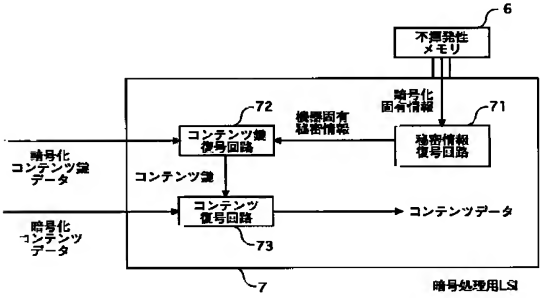
１、８　　秘密情報発行部

2、9	機器製造部	7、14	暗号処理用ＬＳＩ
3、10	変換部	71、142	秘密情報復号回路
4、11	組立部	72、143	コンテンツ鍵復号回路
5、12	ＬＳＩ製造部	73、144	コンテンツ復号回路
6、13	不揮発性メモリ	141	パラメータ記憶手段

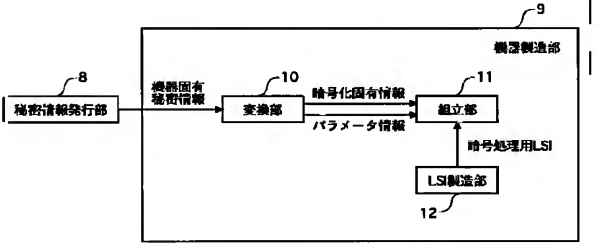
【図1】



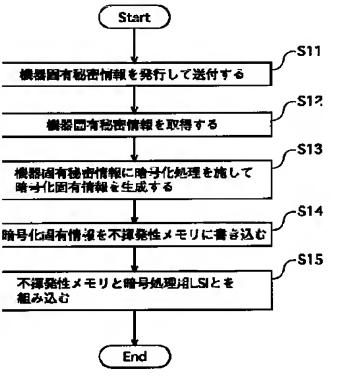
【図2】



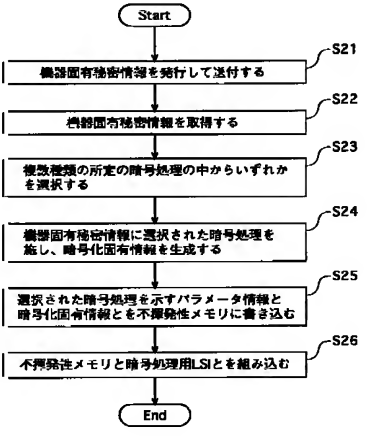
【図4】



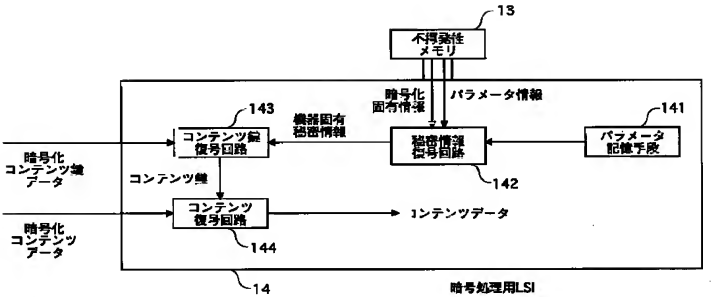
【図3】



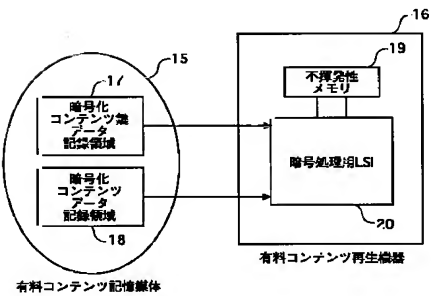
【図6】



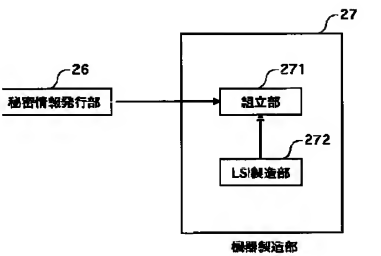
【図5】


13
不揮発性メモリ
暗号化固有情報
パラメータ情報
143
機器固有秘密情報
141
コンテンツ鍵復号回路
秘密情報復号回路
パラメータ記憶手段
暗号化コンテンツ鍵データ
コンテンツ鍵
142
コンテンツ復号回路
コンテンツデータ
暗号化コンテンツデータ
144
14
暗号処理用LSI

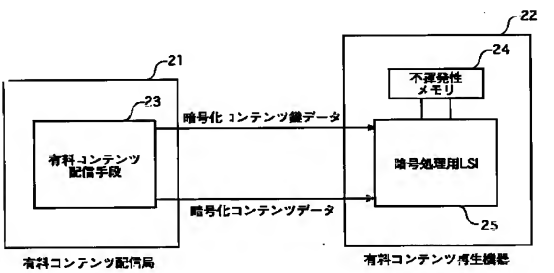
【図7】


16
19
15
17
不揮発性メモリ
暗号化コンテンツ鍵データ記録領域
暗号処理用LSI
暗号化コンテンツデータ記録領域
20
18
有料コンテンツ再生機器
有料コンテンツ記憶媒体

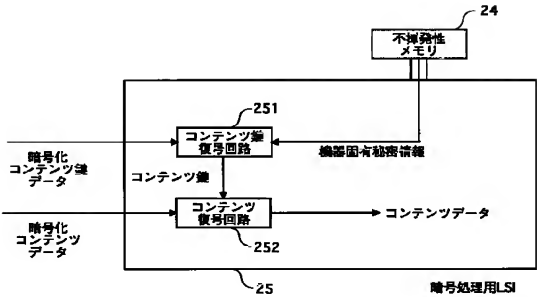
【図10】


27
26
271
秘密情報発行部
組立部
272
LSI製造部
機器製造部

【図8】


22
21
24
不揮発性メモリ
23
暗号化コンテンツ鍵データ
有料コンテンツ配信手段
暗号処理用LSI
暗号化コンテンツデータ
25
有料コンテンツ配信局
有料コンテンツ再生機器

【図9】



フロントページの続き

(72)発明者　井上　信治
大阪府門真市大字門真1006番地　松下電器産業株式会社内

Fターム(参考)　5B017 AA03 AA06 BA07 BB09 BB10 CA05 CA12
5J104 AA12 AA16 EA04 EA26 JA03 KA14 NA02 NA27 NA37 NA39 NA42